SYLLABUS[1]

1. Information about the program

1.1 Higher education institution	Universitatea „Politehnica" din Timişoara
1.2 Faculty[2] / Department[3]	Automatică şi Calculatoare / Automatică și Informatică Aplicată
1.3 Chair	—
1.4 Field of study (name/code[4])	Ingineria Sistemelor
1.5 Study cycle	Master
1.6 Study program (name/code/qualification)	Sisteme Informatice Aplicate in Productie si Servicii

2. Information about the discipline

2.1 Name of discipline			Advanced Techniques for Data and Programs Security				
2.2 Coordinator (holder) of course activities			Assoc. Prof. Bogdan Groza				
2.3 Coordinator (holder) of applied activities [5]			Assoc. Prof. Bogdan Groza				
2.4 Year of study[6]	1	**2.5** Semester	2	**2.6** Type of evaluation	E	**2.7** Type of discipline	Mandatory

3. Total estimated time (hours / semester of didactic activities)

3.1 No. of hrs. / week	3 , of which:	**3.2** course	2	**3.3** seminar/laboratory/ project/training	1
3.4 Total no. of hrs. in the education curricula	32 , of which:	**3.5** course	28	**3.6** applied activities	14

3.7 Distribution of time for individual activities related to the discipline	hrs.
Study using a manual, course materials, bibliography and lecture notes	28
Additional documentation in the library, on specialized electronic platforms and on the field	0
Preparation for seminars / laboratories, homeworks, assignments, portfolios, and essays	14
Tutoring	0
Examinations	0
Other activities	0
Total hrs. of individual activities	32

3.8 Total hrs. / semester[7]	32
3.9 No. of credits	6

4. Prerequisites (where applicable)

4.1 Curriculum	• None
4.2 Competencies	• Computer programming (C++, .NET or Java)

5. Conditions (where applicable)

5.1 of the course	• Lecture room with notebook and beamer
5.2 to conduct practical activities	• Laboratory computers with IDEs for C++, .NET & Java

6. Specific competencies acquired

---

[1] The form corresponds to the Syllabus promoted by OMECTS 5703/18.12.2011 (Annex3).
[2] The name of the faculty which manages the educational curriculum to which the discipline belongs.
[3] The name of the department entrusted with the discipline, and to which the course coordinator / holder belongs.
[4] Fill in the code provided in GD no. 493/17.07.2013.
[5] The applied activities refer to: seminar (S) / laboratory (L) / project (P) / practice/training (Pr).
[6] The year of study to which the discipline is provided in the curriculum.
[7] It is obtained by summing up the number of hrs. from 3.4 and 3.7.

Professional competencies[8]	• Apply knowledge from computer science and information technology in the field of information security and cryptography
Transversal competencies	• Communication skills and team work for projects on systems security

7. Objectives of the discipline (based on the grid of specific competencies acquired)

7.1 General objective of the discipline	• Apply notions from information security and cryptography in home grade or industrial grade information systems
7.2 Specific objectives	• Designing practical applications that embed security and cryptography • Programming cryptography in software or hardware, e.g., Java, .NET, C++

8. Content

8.1 Course	No. of hours	Teaching methods
1. Introduction and historical context. Security objectives, adversaries and attacks.	2	Lecture slides and discussions
2. Cryptographic primitives. Overview of symmetric encryption: DES, 3DES, AES. Overview of hash functions: MD5, SHA1, SHA2, SHA3 and keyed hash functions: NMAC, HMAC. Overview of public key encryptions and digital signatures: RSA, Diffie-Hellman-Merkle, ElGamal, DSA, ECC.	4	Lecture slides and discussions
3. Fundamentals. Mathematical Background. Information Theory. Probability Theory. Number Theory. Complexity Theory.	4	Lecture slides and discussions
4.Advanced concepts in symmetric and assymetric cryptography.	2	Lecture slides and discussions
5.Cryptographic protocols 5.1. Authentication protocols: password based authentication, one-time passwords, challenge-response and zero-knowledge. 5.2. Authentication protocols in practice: NTLM, MS-CHAP, ISO TPMA. 5.3. Authentication protocols in computer networks and over the Internet: EKE, STS, IPSec, SSL/TLS, SSH, Kerkeros. 5.4. E-banking authentication.	6	Lecture slides and discussions
6. Software security 6.1. Cryptography in .NET and Java. 6.2. Digital rights management and software protection: obfuscation, tamper-proofing and watermarking.	4	Lecture slides and discussions
7. Hardware security. 7.1. Smart-card security, the PKCS11 standard. 7.2. Side-channel attacks and countermeasures.	2	Lecture slides and discussions
8. Wireless security. 8.1. The 802.11 security suite: WEP, WPA, WPA2. 8.2. Bluetooth security. 8.3. Security in sensor networks, the TESLA protocol family. 8.4. NFC security.	2	Lecture slides and discussions
9. Automotive security. 9.1. Anti-theft protection: the electronic	2	

[8] The professional competencies and the transversal competencies will be treated according to the Methodology of OMECTS 5703/18.12.2011. The competencies listed in the National Register of Qualifications in Higher Education [Registrul Naţional al Calificărilor din Învăţământul Superior RNCIS] (http://www.rncis.ro/portal/page?_pageid=117,70218&_dad=portal&_schema=PORTAL) will be used for the field of study from 1.4 and the program of study from 1.6 of this form, involving the discipline.

immobilizer. 9.2. The digital tachograph system 9.3. Secure software updates. 9.4. Secure in-vehicle communications		

Bibliography[9]

[1] Bogdan Groza, Introducere in criptografie: functii criptografice, fundamente matematice și computaționale, 200 pagini, ISBN 978-973-625-564-9, 2007.

[3] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 816 pages, ISBN 0849385237 , 1996.

[4] Bruce Schneier, Applied Cryptography, John Wiley & Sons, 784 pages, ISBN 0471117099 , 1996.

[5] Wenbo Mao, Modern Cryptography:Theory and Practice, 648 p., ISBN13:9780130669438, ISBN10: 0-13-066943-1, Prentice Hall, 2003.

[6] Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley, 640 p., ISBN 0-471-38922-6, 2001.

[7] Matt Bishop, Computer Security: Art and Science, 1136 p., Addison-Wesley Professional, ISBN-10: 0201440997, ISBN-13: 978-0201440997, 2002.

[8] Peter Thorsteinson, G. Gnana Arun Ganesh, .NET Security and Cryptography, 496 pages, Prentice Hall (August 28, 2003), ISBN-10: 013100851X, ISBN-13: 978-0131008519

[9] Brian A. LaMacchia, Sebastian Lange, Matthew Lyons, Rudi Martin, Kevin T. Price, .NET Framework Security, Addison Wesley, 2002, ISBN : 0-672-32184-X, 816 p.

[10] François Koeune, and François-Xavier Standaert. A Tutorial on Physical Security and Side-Channel Attacks, Foundations of Security Analysis and Design III : FOSAD 2004/2005, Volume 3655 of Lecture Notes in Computer Science, pages 78-108, November 2006

[11] Kerstin Lemke , Christof Paar, Marko Wolf et al., Embedded Security in Cars: Securing Current and Future Automotive IT Applications, 273 pages, Springer; 1 edition (December 7, 2005), ISBN-10: 3540283846, ISBN-13: 978-3540283843.

[12] Donggang Liu, Peng Ning, Security for Wireless Sensor Networks, 212 pages, Springer; 1 edition (November 9, 2006), ISBN-10: 0387327231, ISBN-13: 978-0387327235

[13] Praphul Chandra, Bulletproof Wireless Security (GSM, UMTS, 802.11 and AdHoc Security), ISBN: 0-7506-7746-5, Elsevier, 2005.

8.2 Applied activities[10]	No. of hours	Teaching methods
Implementation on an embedded device, e.g., microcontroller, smart-card, etc., of a small security application, e.g., authentication protocol, cryptographic primitive, etc.	28	Open discussions with the students
I		

[9] At least one title must belong to the department staff teaching the discipline, and at least 3 titles must refer to national and international works relevant for the discipline, and which can be found in the Politehnica University Library.

[10] The types of applied activities are those specified in footnote 5. If the discipline contains several types of applied activities, then these will be written consecutively in the lines of the table below. The type of activity will be written in a distinct line, as „Seminar:", „Laboratory:", „Project:" and/or „Practice/Training:".

Bibliography [11]

[1] Ross Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley, 640 p., ISBN 0-471-38922-6, 2001.
[2] Peter Thorsteinson, G. Gnana Arun Ganesh, .NET Security and Cryptography, 496 pages, Prentice Hall (August 28, 2003), ISBN-10: 013100851X, ISBN-13: 978-0131008519
[3] Brian A. LaMacchia, Sebastian Lange, Matthew Lyons, Rudi Martin, Kevin T. Price, .NET Framework Security, Addison Wesley, 2002, ISBN : 0-672-32184-X, 816 p.

9. Corroboration of the content of the discipline with the expectations of the main representatives of the epistemic community, professional associations and employers in the field afferent to the program

- University of Bristol http://www.cs.bris.ac.uk/Teaching/unitglance.jsp?unit=COMS30002
-

10. Evaluation

Type of activity	**10.1** Evaluation criteria	**10.2** Evaluation methods	**10.3** Share of the final grade
10.4 Course	Scoring at least 5 out of 10 points in the evaluation	Written exam	2/3
10.5 Applied activities	**S:**		
	L: Scoring at least 5 out of 10 points in the evaluation	Laboratory tests	1/3
	P:		
	Pr:		
10.6 Minimum performance standard (minimum amount of knowledge necessary to pass the discipline and the way in which this knowledge is verified)			
• Minimal knowledge of security protocols and cryptography			

Date of completion	**Course coordinator (signature)**	**Coordinator of applied activities (signature)**
29.06.2015	.....	.....
Head of Department (signature)	**Date of approval in the Faculty Council[12]**	**Dean (signature)**
.....		.....

[11] At least one title must belong to the staff teaching the discipline.
[12] Avizarea este precedată de discutarea punctului de vedere al board-ului de care aparţine programul de studiu cu privire la fişa disciplinei.